General Policy

DATA BREACH

Intent Cairns Regional Council (Council) recognises the significant responsibility that comes with handling personal information and is committed to protecting it at all times. To support strong information governance practices and to meet Council's obligations under the *Information Privacy Act 2009* and the Mandatory Notification of Data Breach (MNDB) scheme, Council has established a Data Breach Policy. This policy outlines how Council prepares for, identifies, assesses, contains, notifies, and reviews data breaches involving information in Council's possession or control.

Scope Applies to Councillors, Council employees, volunteers, and contractors and contracted service providers handling Council information under service arrangements.

DEFINITIONS

Term	Meaning
Affected individual	An "affected individual" under section 47(1)(ii) of the IP Act is an individual to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.
Councillors	All elected representatives who hold (current) office with council, including the mayor.
Data breach	The unauthorised access to, or unauthorised disclosure of information or the loss of information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur in accordance with schedule 5 of the IP Act.
Data Breach Response Plan	A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing Council's more specific processes in managing and responding to a data breach.
Eligible Data Breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: (a) there has been unauthorised access to, or unauthorised disclosure of personal information held by Council, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or (b) there has been loss of personal information held by Council that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.
Information Commissioner	The Queensland Information Commissioner. The Office of the Information Commissioner is Queensland's independent body that oversees the administration of right to information and information privacy laws, ensuring

Term	Meaning
	agencies comply with their obligations and protecting the personal information of the community.
IP Act	The *Information Privacy Act 2009* (Qld).
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (a) whether the information or opinion is true or not, and (b) whether the information or opinion is recorded in a material form or not.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or (b) serious harm to the individual's reputation because of the access or disclosure.

PROVISIONS

Principles

Council is committed to protecting personal information and ensuring strong data governance. This policy aims to safeguard the privacy of individuals, protect Council information and minimise harm resulting from data breaches. Effective breach management helps reduce impacts on affected individuals and organisations, while also enabling Council to learn from incidents and strengthen its data protection measures.

Data Breach

A 'data breach' for the purpose of this policy means either of the following in relation to personal information held by Council:

- unauthorised access to, or unauthorised disclosure of, the information.
- the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.

A data breach may occur through malicious or criminal activity, system faults, or human error, and can involve unauthorised access, unauthorised disclosure, or the loss of information where unauthorised access or disclosure is likely to occur.

<u>Malicious or criminal attack:</u>

- Cyber incidents such as ransomware, malware, hacking, phishing or credential-harvesting attempts that result in unauthorised access to, leakage of or theft of personal information.
- Social engineering or impersonation that tricks staff into inappropriately providing personal information to unauthorised individuals.
- Insider threats, where an employee or contractor intentionally abuses valid system access to view, use or disclose personal information beyond their delegated role or permissions.
- Theft or loss of physical assets containing personal information, such as laptops, mobile phones, USB drives, paper files or removable media.

System fault:

- System failures or configuration issues can inadvertently expose personal information.
- Software bugs or configuration errors that allow unintended system access without authentication or automatically generate correspondence containing the wrong personal information.
- Incorrect publication of information, such as a database, internal portal or document accidentally being made publicly accessible online.
- Automated notices (e.g., infringement notices, development application updates) being sent to incorrect recipients due to a system error.

Human error:

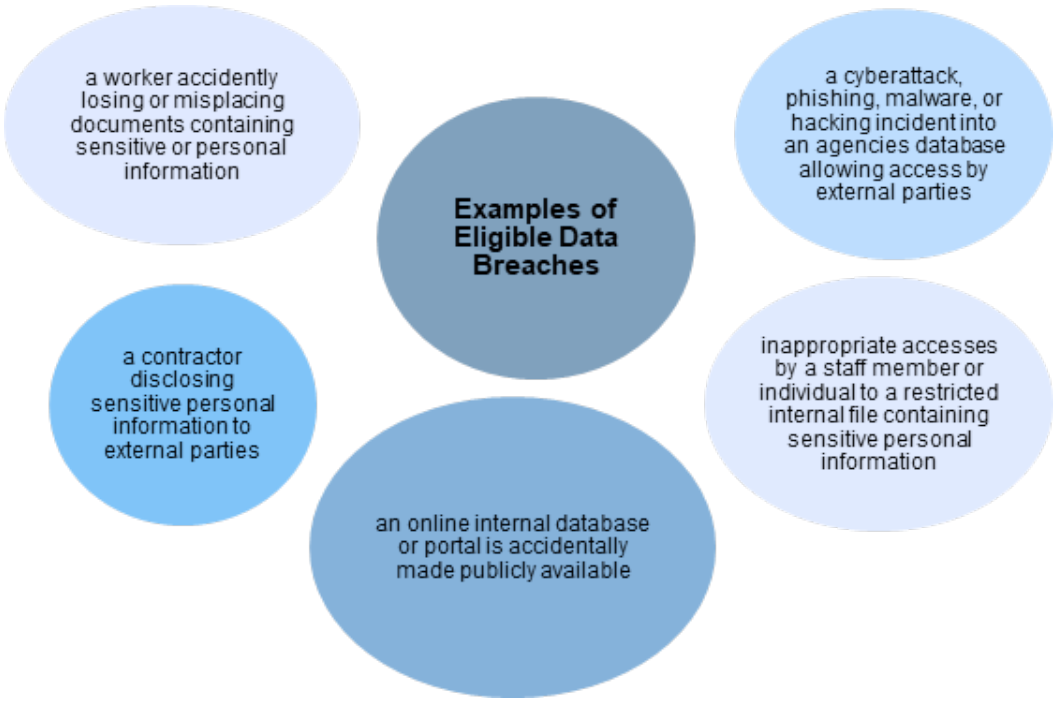
- Emailing or mailing information to the wrong recipient, including where attachments contain personal information not intended to be shared.
- Incorrect access permissions, where an employee or contractor is unintentionally granted access to systems or folders containing personal or sensitive information.
- Poor password or security practices, including sharing login credentials, not securing files, or failing to review or remove access when roles change.
- Accidentally losing or misplacing documents containing personal information, such as development application paperwork or complaint files.

Eligible Data Breach

A data breach becomes an Eligible Data Breach when it involves personal information likely to result in serious harm, such as financial, psychological or reputational harm. This includes situations where there has been actual unauthorised access or disclosure, as well as cases where information is lost and it is reasonably likely that such access or disclosure will occur.

In the event of a data breach Council is required to comprehensively assess the risks associated with the breach. As the *Information Privacy Act 2009* (IP Act) imposes specific obligations for an Eligible Data Breach, a Data Breach Policy needs to detail Council's assessment process for any data breach but also the process for specifically determining whether the data breach is an Eligible Data Breach for the purposes of the IP Act and the Mandatory Notification of Data Breach (MNDB) scheme.

Examples of Eligible Data Breaches. *Source: Office of the Information Commissioner*.



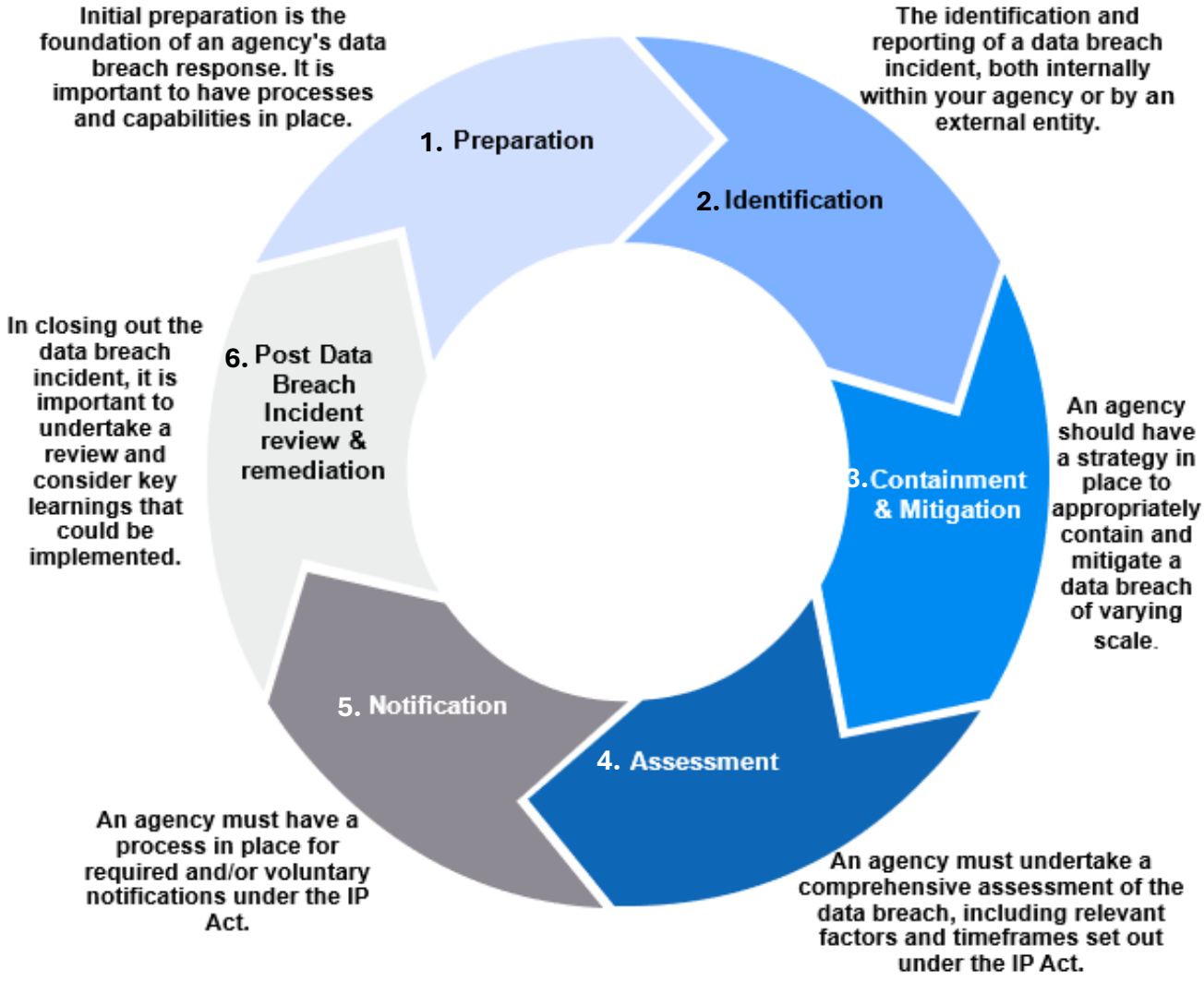
Data Breach Readiness, Response and Reporting

Council recognises that every data breach requires careful assessment and a response that fits the specific circumstances. Readiness involves maintaining up-to-date policies, procedures and internal registers, supported by trained staff who understand their roles in assessing and containing a breach.

To support clarity and consistency in how incidents are handled, Council follows six core stages that guide our readiness and our approach to assessing, containing, managing and resolving a breach.

Council's internal data breach response plan outlines the actions that will be taken when a data breach occurs and provides a structured process to ensure incidents are managed effectively and responsibly.

Six Stages that Support Readiness, Response and Reporting. *Source: Office of the Information Commissioner.*



Stage 1: Preparation

Council will:

- Maintain this Policy, a Data Breach Response Plan, and Cyber Incident Response Plan and Data Breach Incident Response Playbook.
- Build organisational capability through training and simulations.
- Integrate data breach management with risk, ICT security and business continuity frameworks.

Stage 2: Identification

Council will:

- Recognise potential breaches from internal or external sources, including contractors, other agencies or the public.
- Triage and escalate potential data breaches promptly.
- Consider whether the incident could be an Eligible Data Breach involving personal information by assessing the data breach to make a preliminary assessment of the risk posed by the breach
- Coordinate response as required to ensure an effective and timely management of the breach.

Stage 3: Containment and mitigation

Council will:

- Take immediate reasonable steps to stop further unauthorised access or disclosure and to recover information where possible.
- Apply proportionate controls, for example suspending access, revoking credentials, isolating systems, recalling emails or contacting unintended recipients.
- Commence a preliminary risk appraisal covering information sensitivity, scale and potential impacts to individuals.

Stage 4: Assessment

Council will:

- Where there is a reasonable suspicion of an Eligible Data Breach, complete an assessment within 30 days to decide if there are reasonable grounds to believe the breach is eligible. Extensions may be used only as permitted by the IP Act.
- Consider statutory serious harm factors, document decisions and preserve evidence.
- Decide on any need to engage external forensic or legal expertise.

Stage 5: Notification

Council will:

- Notify the OIC and affected individuals as soon as practicable if Council knows or assesses the breach as an Eligible Data Breach and no exemption applies.
- Notify the OIC by written statement with required information.
- Appropriately notify individuals impacted by an Eligible Data Breach. If individual contact is not reasonably practicable, Council will publish required information on its website for at least 12 months and advise the OIC how to access the notice.

Stage 6: Post-incident review and remediation

Council will:

- Conduct a structured lessons-learned review, assign actions and track remediation to completion.
- Update practices, systems, training and contracts as required.
- Ensure a complete record of the incident and response is captured in line with obligations under the *Public Records Act 2023*.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Councillors, Council employees, volunteers, and contractors and contracted service providers handling Council information under service arrangements.	• Comply with the Data Breach Policy and understand what is expected of them. • Comply with the IP Act, including protecting personal information held by the Council from unauthorised access, disclosure or loss. • Where required in accordance with this Data Breach Policy, immediately report a data breach or suspected data breach to the appropriate officer including your supervisor or manager, Information and Technology Services and/or the Information Governance Unit. • Respond to requests for information from and cooperate with the Privacy Officer and Information and Technology Services as required. • Comply with recordkeeping obligations.
Delegated Privacy Officer	• Assess the severity of a data breach involving personal information and the likelihood that a breach will result in serious harm to an individual to whom the information involved relates. • Escalate serious data breaches to Executive Manager Information and Technology Services and Director People and Organisational Performance. • Notify the Information Commissioner, affected persons and others where required. This includes publishing, monitoring and reviewing the currency of public notifications of a data breach published to the Council website under section 53(1)(c) of the IP Act. • Immediately report a data breach that is also a cyber security incident to the Executive Manager Information and Technology Services, if not already reported. • Maintain the Register of Eligible Data Breaches.
Supervisors and Managers	• Identify and escalate concerns within your area of responsibility that may trigger the requirements of this Data Breach Policy. • Immediately report a data breach that is also a cyber security incident to the Executive Manager Information and Technology Services, if not already reported.

Role	Responsibility
Executive Manager Information and Technology Services	• Immediately report a cyber security incident that is also a data breach to Council's Privacy Officer, if not already reported. • Implement the Cybersecurity Management Plan and related procedures if the data breach is also a cyber security incident. • Escalate matters to the Business Continuity Team (BCT), when appropriate.

RELATED DOCUMENTS

Information Privacy General Policy
Information Security Management Administration Instruction
Data Breach Response Plan

◆◆◆◆◆◆

This policy is to remain in force until otherwise determined by Council.

Director responsible for Review: **Director People and Organisational Performance**

ORIGINALLY ADOPTED: 27/05/2026
CURRENT ADOPTION: 27/05/2026
DUE FOR REVISION: 27/05/2030
REVOKED/SUPERSEDED:

Ken Gouldthorp.

.....
Ken Gouldthorp
CHIEF EXECUTIVE OFFICER